Proceedings

The Computer Security Foundations Workshop III
Proceedings

The Computer Security Foundations Workshop III

June 12-14, 1990

The Franconia Inn
Franconia, New Hampshire

IEEE Computer Society Press
Los Alamitos, California

Washington ● Brussels ● Tokyo
# Table of Contents

Preface .......................................................... v

## LOGIC AND PROTOCOL ANALYSIS

A Logic for Reasoning About Security .......................... 2
   J. Glasgow, G. MacEwen, and P. Panangaden
A Logic of Communication in Hostile Environment ............ 14
   P. Bieber
Representing Partial Knowledge in an Algebraic Security Model .................................. 23
   C. Meadows
Formal Semantics for Logics of Cryptographic Protocols ......... 32
   P. Syverson

## MODELS OF INFORMATION FLOW

Categorising Non-interference ................................ 44
   J. Jacob
Petri Net Based Modelling of Information
Flow Security Requirements ...................................... 51
   V. Varadharajan
Secure Information Flow Using Security Groups ................. 62
   S.N. Foley

## INFORMATION FLOW IN ABSTRACT MACHINES

Quotient States and Probabilistic Channels .................. 74
   I.S. Moskowitz
Hookup Security for Synchronous Machines ................... 84
   J.K. Millen
Security Models for Priority Buffering and Interrupt Handling ........................................... 91
   D. Rosenthal
A CSP Formulation of Noninterference and Unwinding ........... 98
   P. Ryan

## MODELING NEW PROPERTIES

Formal Modeling in a Generalized Framework for Access Control .................................. 100
   L.J. La Padula
A Policy Model for Denial of Service .......................... 110
   E. Amoroso
Providing a Flexible Security Override for Trusted Systems ........................................ 115
   L. Badger

## COVERT CHANNEL ANALYSIS

The Serial Product of Controlled Signalling Systems:
A Preliminary Report ........................................... 124
   J. Trostle
Networks of Covert Channels .................................. 125
   T. Wittbold
COVERT CHANNEL DETECTION

Information Sharing in Secure Systems .............................................. 128
   J.W. Gray, III
Information-Flow Analysis for Covert-Channel Identification in
Multilevel Secure Operating Systems .............................................. 139
   J. He and V.D. Gligor
A Methodology for the Detection of Timing Channels ......................... 149
   J.C. Wray

DATABASE SECURITY

A Formal Framework for Single Level Decomposition of
Multilevel Relations ................................................................. 152
   S. Jajodia and R. Sandhu
A New Polyinstantiation Integrity Constraint for Multilevel Relations .... 159
   R. Sandhu, S. Jajodia, and T. Lunt
Recursion Theoretic Properties of the Inference Problem in
Database Security ........................................................................ 166
   M.B. Thuraisingham

Author Index ...................................................................................... 167